The information security incident notification scheme (**the scheme**) provides tangible resources, trends analysis and risk reporting.

Overview of this report

The Incident Insights Report provides a summary and analysis of the information security incident notifications received by OVIC between **1 July 2020** to **31 December 2020**.

Our observations and take-outs in this report are based on comparing the statistics previous published in the [Incident Insights Report for 29 October 2019 – 30 June 2020](https://ovic.vic.gov.au/data-protection/security-insights/incident-insights-report29-october-2019-30-june-2020/) with the notifications received by our office between July – December 2020. We acknowledge these are different lengths of time as we enter more regular reporting cycles.

Victoria Police incident statistics are reported on an annual basis consistent with existing reporting commitments. For their latest incident statistics refer to OVIC’s [Incident Insights Report for 29 October 2019 – 30 June 2020](https://ovic.vic.gov.au/data-protection/security-insights/incident-insights-report29-october-2019-30-june-2020/).

Information security incident notification insights from July 2020 – December 2020

Notifications by month

A graph of a number of columns

Description automatically generated with medium confidence

OVIC received 155 notifications between 1 July 2020 to 31 December 2020 (inclusive). This represents double the number of notifications compared to the last reporting period.

We received the highest number of notifications in November 2020. This does not necessarily reflect more incidents occurring during this month, as some agencies provided multiple months’ worth of notifications to us at one time. For this reason, caution should be observed drawing conclusions from month-to-month comparisons.

**Takeout:**   
*As predicted in the previous report, notifications have steadily increased (78 in the last reporting period compared to 155 this period) as awareness of the scheme increases across the VPS.*

*The decline in notifications in December 2020 does not necessarily reflect less incidents occurring and could be a result of organisations focussing on completing other business priorities before the end of year.*

Notifications by portfolio

A pie chart with numbers and text

Description automatically generated

Of the 155 notifications received by OVIC, the majority came from the Justice and Health and Human Services sectors. This follows a similar trend observed in the Oct 2019 – Jun 2020 report.

We received notifications from the Jobs, Precincts and Regions portfolio for the first time during this reporting period.

The Education sector had the largest increase in notifications compared to the last report, followed by the Treasury and Finance and Health and Human Services sectors.

**Takeout:** *A greater representation of information security incident notifications across all sectors, is a welcome development. This is likely a reflection of greater awareness about the scheme It may also reflect increased awareness and identification of information security incidents as they occur and more streamlined reporting procedures in individual organisations.*

While we received a higher number of notifications from some sectors, the statistics do not necessarily mean that these portfolios have the most incidents. Instead, the number of notifications may indicate that these portfolios have greater awareness of the scheme, resources to identify and analyse incidents, and a willingness to report to OVIC. In addition, because more agencies are now reporting (e.g., DJPR) the increased number of incidents does not mean a decrease in the security of the VPS overall.

Information format

A blue rectangle with a bar code

Description automatically generated

Similar to the previous six months, the majority of incident notifications related to electronic information followed by hard copy information.

Of the notifications relating to information in electronic format, approximately 65% of incidents related to emails. These incidents were either related to phishing, incorrect recipients, incorrect attachments, compromised email accounts or not using the BCC field to send emails to a large number of recipients.

OVIC receives notifications in different forms and not always through the incident notification form published on our website. As a result, we were unable to ascertain the format of the affected information in one of the notifications*.*

**Takeout:** *Although it is not readily apparent in the statistics when presented as percentages, there was an increase in notifications affecting hard copy information and verbal disclosures.*

*The increase in notifications related to incidents other than electronic information demonstrates an increasing level of maturity by the VPS in this space.*

Type of information impacted

A colorful circle with text

Description automatically generated

Most notifications received by OVIC related to compromises of personal information, followed by health information.

Compared to the last reporting period, notifications related to personal information increased from 63% to 81%.

There was also a decrease in the number of incident notifications relating to operational information from 9% in the last reporting period to 3% this reporting period.

**Takeout:**   
*OVIC published some follow up guidance regarding this field in its* [*January 2021 newsletter*](https://mailchi.mp/f81a1d6d1dca/ovic-newsletter-january21?e=%5bUNIQID%5d) *to spotlight the types of information OVIC accepts notifications for given VPS organisations handle a broad range of information.*

Information business impact level

*A blue and pink squares

Description automatically generated*

Most notifications received by OVIC were for BIL 2 information, consistent with the last reporting period.

OVIC received a number of notifications through the privacy data breach reporting form which collects different information. As a result there was an increase from 1% to 14% of notifications received that did not identify the BIL of the information affected.

**Takeout:**   
*OVIC is reviewing the notification scheme after a year of operation to see where improvements can be made.*

*Notifying OVIC of information security incidents regardless of impact level provides us with greater insights to share with the VPS and informs the development of training and awareness material.*

Potential business impact category affected

A blue circle with different colored numbers

Description automatically generated

Given the majority of notifications related to personal information, the most commonly selected BIL category was ‘personal*’,* as the compromise was assessed to have the potential to cause harm to an individual.

**Takeout:**   
*OVIC is planning to publish some guidance in the* [*monthly newsletter*](https://ovic.vic.gov.au/monthly-newsletters/) *by spotlighting certain fields each month, and what organisations should consider when completing each field.*

Security attributes impacted

*A blue circle with pink and purple circles

Description automatically generated*

While the number of notifications received relating to compromises in the confidentiality of public sector information doubled, the percentage compared to other security attributes remained consistent with the last reporting period.

**Takeout:**   
*Accidentally sending an email to the wrong recipient continues to be the leading cause of confidentiality related incident notifications. In fact, email disclosure makes up almost 30% of incident notifications received. OVIC recently published guidance on* [*Tips to reduce data breaches when sending emails*](https://ovic.vic.gov.au/resource/tips-to-reduce-data-breaches-when-sending-emails/) *published on our website.*

*In the Office of the Australian Information Commissioner’s (****OAIC****) Jul - Dec 2020 Notifiable Data Breaches Report[[1]](#footnote-1) human error was attributed to 38% of notifications to their office during the same period.*

Security areas affected

A blue and white flag

Description automatically generated

There continues to be a high number of notifications received that nominate ‘information’ as the security area affected.

‘Information’ as a security area refers to the process of valuing public sector information and applying protective markings. An example of an incident affecting the ‘information’ security area might the inappropriate application of a protective marking on information.

**Takeout:**   
*Some notifications suggested that ‘information’ had been selected simply because the organisation was submitting an information security incident notification. Selecting the security area of ‘information’ is not wrong (considering the reporting context), but a more helpful insight would be understanding what particular security control failed, and the associated security area of this control i.e., an individual disclosed information that they should not have, which relates to the personnel security area.*

*OVIC published some follow up guidance regarding this field in its* [*February 2021 newsletter*](https://mailchi.mp/f8d28c940e6d/ovic-newsletter-feb?e=%5bUNIQID%5d) *to spotlight the available options under this field and provide an explanation of each area.*

**Note**: Whole number percentage values have been used for readability and are approximate.

Risk statements

Based on the incident notifications received by OVIC, we have developed the following risk statements for consideration by VPS organisations when reviewing their information security risks:

| The risk of… | Caused by… | Resulting in…[[2]](#footnote-2) |
| --- | --- | --- |
| Unauthorised disclosure of client information  *(Compromise of confidentiality)* | Employees accidentally attaching incorrect documents to emails (e.g., related to another matter) | Impact to individuals whose personal information was affected |
| Inappropriate handling of identity documents  *(Compromise of confidentiality and integrity)* | Employees failing to follow the quality assurance process and mailing documents to incorrect recipient | Impact to individuals whose personal information was affected |
| Inability to access customer records when required  *(Compromise of availability)* | Incorrect access controls being applied by administrator during a cloud migration of an ICT system | Impact to service delivery |
| Unauthorised disclosure of staff information  *(Compromise of confidentiality)* | Third party inadvertently using ‘live’ production data instead of dummy data in a test environment | Impact to individuals whose personal information was affected |
| Unauthorised access and use of operational information  *(Compromise of confidentiality)* | Malicious employee sending operational information to their own personal email address or storage provider (e.g., Dropbox, One drive etc.) | Impact on public services (reputation of, and confidence in, the organisation) |

More information

For further information on the information security incident notification scheme and to download a notification form, visit our website:  
<https://ovic.vic.gov.au/data-protection/agency-reporting-obligations/incident-notification/>

We welcome your feedback on this report. Contact OVIC at [security@ovic.vic.gov.au](mailto:security@ovic.vic.gov.au) if you would like to discuss this report any further.

1. Refer to OAIC’s website for a copy of their Jul-Dec report <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2020/> [↑](#footnote-ref-1)
2. The extent of the impact could be “limited” or higher depending on the context and nature of the incident and is left for an organisation to determine. [↑](#footnote-ref-2)